

ACISP 2022

Hybrid Dual and Meet-LWE Attack

BI Lei^{1,2}, LU Xianhui^{1,2,3}, LUO Junjie⁴, WANG Kunpeng^{1,2}

1. Institute of Information Engineering, CAS
2. School of Cyber Security, University of Chinese Academy of Sciences
3. State Key Laboratory of Cryptology
4. Beijing Jiaotong University

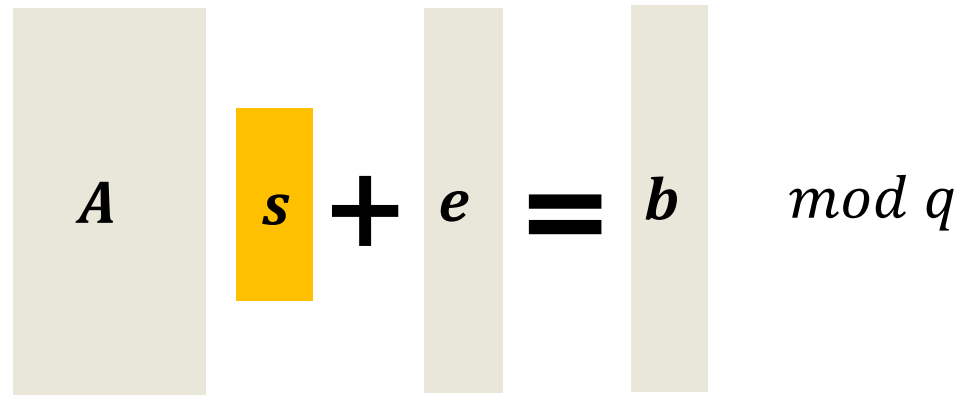


Outline

- **Background**
- **Recall hybrid dual attack and Meet-LWE attack**
- **Hybrid dual and Meet-LWE attack**
- **Concrete security estimation of FHE**
- **Conclusion**

Background

- **LWE (Learning with errors) problem** [Regev05]

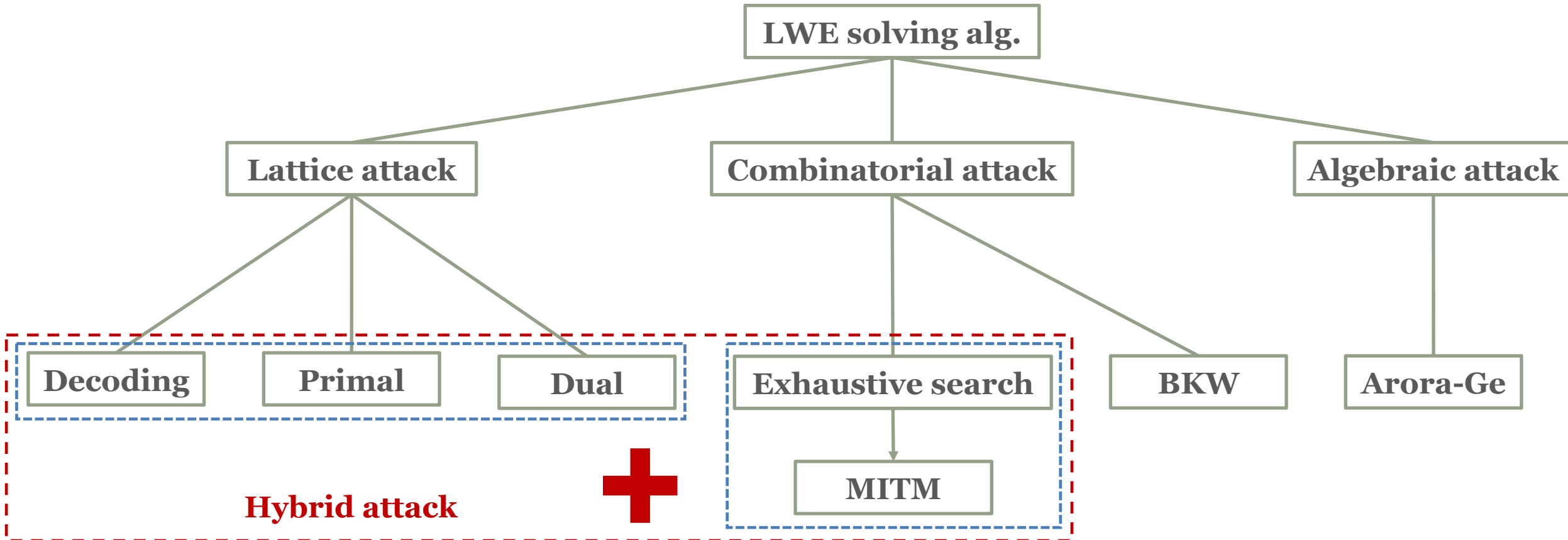

$$A + s + e = b \mod q$$

Given (A, b)

- **Search-version** : find s
- **Decision-version** : LWE or Uniform dist. ?

Background

- LWE solving algorithms



Recall Hybrid Dual Attack

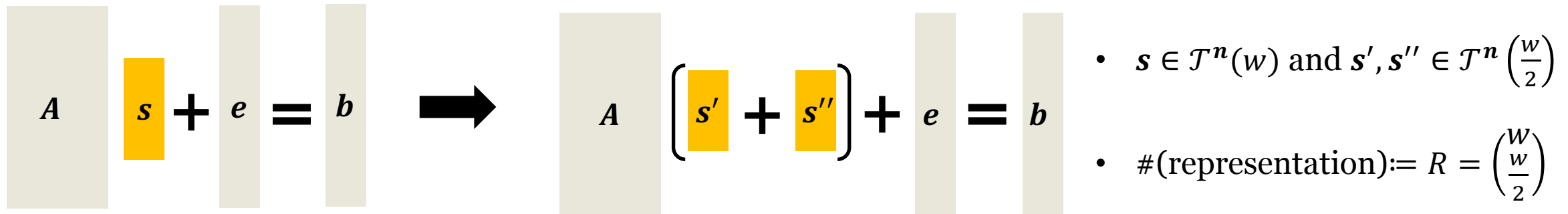
$$\left[\begin{array}{c} \boxed{w} \quad \left(\begin{array}{c|c} A_1 & A_2 \end{array} \right) \begin{array}{c} s_1 \\ s_2 \end{array} + e = b \end{array} \right] \mod q \quad (w, v) \leftarrow \Lambda^\perp(A_2) = \{(w, v) | wA_2 = v \mod q\}$$

$$\underbrace{\boxed{w} \quad A_1}_{\hat{a}} \quad \underbrace{\begin{array}{c} s_1 \\ v \end{array} \quad s_2}_{\hat{e}} + \underbrace{\boxed{w} \quad e}_{\hat{b}} = \boxed{w} \quad b \mod q$$

Guess s_1 \dashrightarrow hypothesis test on $\hat{b} - \langle \hat{a}, s_1 \rangle \mod q$ \dashrightarrow $\left\{ \begin{array}{l} \text{modular Gaussian} \Leftrightarrow \text{Correct} \\ \text{uniform} \end{array} \right.$

Recall Meet-LWE Attack

- Meet-LWE attack on sparse ternary LWE [May21]

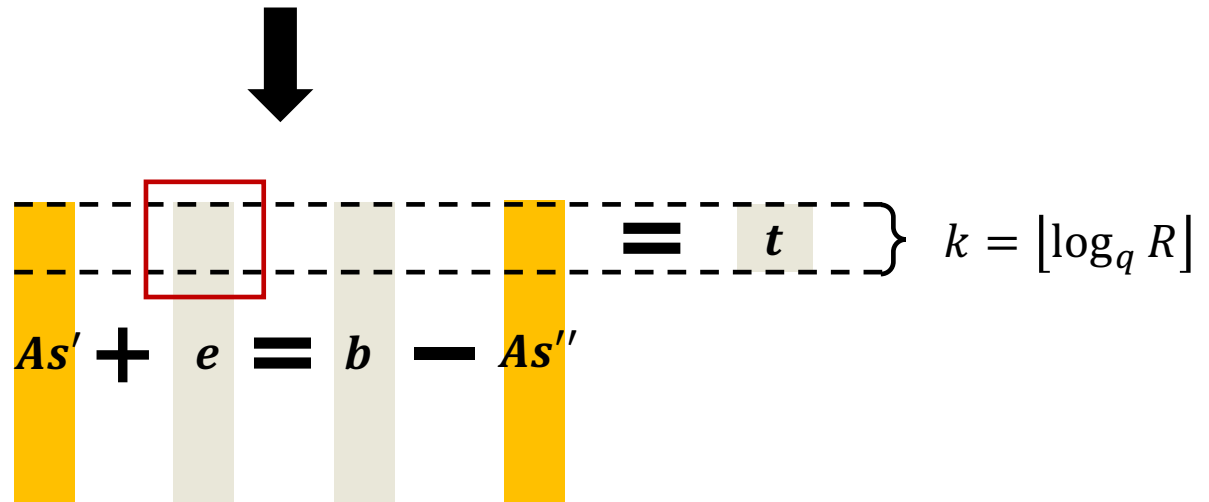


$$A \cdot s + e = b \quad \longrightarrow \quad A \cdot (s' + s'') + e = b$$

- $s \in \mathcal{T}^n(w)$ and $s', s'' \in \mathcal{T}^n\left(\frac{w}{2}\right)$
- $\#(\text{representation}) := R = \binom{W}{\frac{w}{2}}$

- $L_1 = \left\{ s' \in \mathcal{T}^n\left(\frac{w}{2}\right) \mid \pi_k(As' + e) = t \right\}$

- $L_2 = \left\{ s'' \in \mathcal{T}^n\left(\frac{w}{2}\right) \mid \pi_k(b - As'') = t \right\}$



$$As' + e = b - As''$$

$$\left. \begin{array}{c} \text{---} \boxed{\text{---}} \text{---} \end{array} \right\} \pi_k(\text{---}) = t \quad k = \lfloor \log_q R \rfloor$$

Recall Meet-LWE Attack

- **Meet-LWE attack on sparse ternary LWE** [May21]

- **compute** $k = \lfloor \log_q R \rfloor$ **and fix a** $t \xleftarrow{\$} \mathbb{Z}_q^k$
- **For each** $\pi_k(e) \in \mathcal{T}^k$ **do**
 - **construct** $L_1 = \left\{ \left(s' \in \mathcal{T}^n \left(\frac{w}{2} \right), h(As' + e) \right) \mid \pi_k(As' + e) = t \right\}$
 - **construct** $L_2 = \left\{ \left(s'' \in \mathcal{T}^n \left(\frac{w}{2} \right), h(b - As'') \right) \mid \pi_k(b - As'') = t \right\}$
- **For all matched** (s', \cdot) **and** (s'', \cdot) **in the 2nd component do**
 - **if** $s = s' + s'' \in \mathcal{T}^n(w)$ **and** $As - b \in \mathcal{T}^k$ **then**
 - **return** s

Hybrid Dual and Meet-LWE Attack

- Use Meet-LWE attack to accelerate guessing s_1

$$A \cdot s + e = b \quad \longrightarrow \quad \underbrace{w \cdot A_1}_{\hat{a}} \cdot s_1 + \underbrace{v \cdot s_2 + w \cdot e}_{\hat{e}} = \hat{b}$$

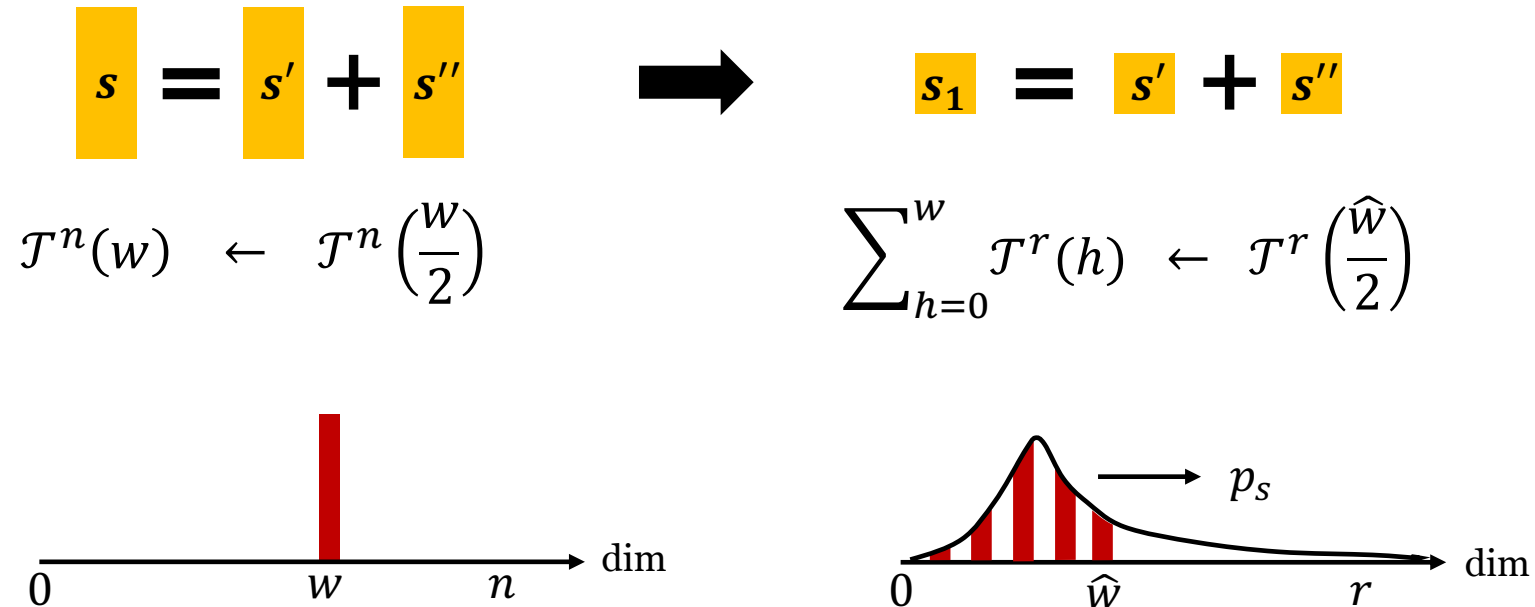
- Dual attack makes a **trade-off** between the dim of secret and the norm of error

Technical problems

1. **secret** : hamming weight fixed \rightarrow unknown
2. **error** : ternary \rightarrow large

Hybrid Dual and Meet-LWE Attack

- Problem 1 --- unknown hamming weight of the secret



Hybrid Dual and Meet-LWE Attack

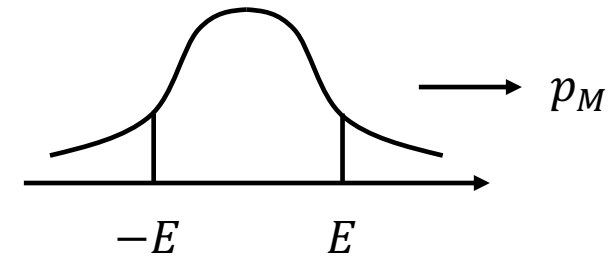
- Problem 2 --- large error

$$\hat{e} = \begin{matrix} v \end{matrix} \begin{matrix} s_2 \end{matrix} + \begin{matrix} w \end{matrix} \begin{matrix} e \end{matrix} \sim \mathcal{G}_\rho \gg e$$

- Enumerate $\{-E, \dots, E\}$ instead of $\{-1, 0, 1\}$

$$\begin{matrix} As' \end{matrix} + \begin{matrix} e \end{matrix} = \begin{matrix} b \end{matrix} - \begin{matrix} As'' \end{matrix} \quad \left. \begin{matrix} \text{---} \\ \text{---} \end{matrix} \right\} k$$

Diagram illustrating the equation $As' + e = b - As''$ with a red box highlighting the error term e . The terms are represented by colored bars: yellow for As' and As'' , and grey for e and b . A dashed line with a bracket labeled k spans the width of the equation.



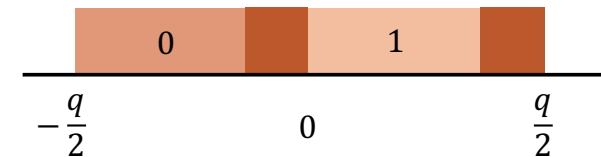
Hybrid Dual and Meet-LWE Attack

- Problem 2 --- large error

$$\hat{e} = \boxed{v} \boxed{s_2} + \boxed{w} \boxed{e} \sim \mathcal{G}_\rho \gg e$$

- Define a new hash function

$$h(x_i) = \begin{cases} 0, & x_i \in \left[-\frac{q}{2}, -E\right) \\ 1, & x_i \in \left[0, \frac{q}{2} - E\right) \\ 0, 1, & x_i \in [-E, 0) \cup \left[\frac{q}{2} - E, \frac{q}{2}\right) \end{cases}$$



$$\#(\text{addresses for each element}) = 2^{\frac{2E+1}{q} \cdot M}$$

Concrete Security Estimation of FHE

- Improvements up to **16 bits**

200										103	120	131
160		OURS								117	146	161
120		HYBRID1								136	182	202
100		HYBRID2					102	124	133	147	199	230
80							119	146	162	162	225	276
60				90	106	111	134	179	207			
50				101	126	133	146	202	241			
40	76	83	86	115	153	166	163	234	287			
30	95	110	115	138	193	217						
20	128	161	175									
15	153	205	230									
$\log q$ w	64	128	192	64	128	192	64	128	192	64	128	192
$\log n$	10			11			12			13		

200											191	206	207
160											169	174	181
120											157	182	207
100													
80										118	127	133	155
60										119	146	162	165
50													
40													
30													
20													
15													
log n	64	128	192		64	128	192		64	128	192		64
k log n	10				11				12				13

Figure 1 is a heatmap showing the number of reads for each combination of $\log n$ (x-axis) and $\log k$ (y-axis) for the Hybrid method. The x-axis ranges from 6 to 15, and the y-axis ranges from 20 to 200. The heatmap shows a diagonal pattern of green cells, indicating that the number of reads is highest for combinations where $\log n$ and $\log k$ are close. The values range from 84 to 230.

[illegible]

- **HYBRID1 [BLLWZ22]** Hybrid dual attack on LWE with arbitrary secrets. **Cybersecurity 2022.**
- **HYBRID2 [CHHS19]** A hybrid of dual and meet-in-the-middle attack on sparse and ternary secret LWE. **IEEE Access 2019.**

Conclusion

- **Summary**
 - Use Meet-LWE to accelerate guessing in hybrid dual attack
 - Improve the estimation of the concrete security of FHE up to 16 bits
- **Future work**
 - Remove enumerating \hat{e}
 - Replace the hash function

Thanks!